DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on an Altered System of Records
Under the Privacy Act of 1974

1. System identifier and name: DHRA XX, entitled "DoD Sexual Assault Prevention and Response Office Victim Assistance Data Systems."

2. Responsible official: Ms. Bette Inch, Senior Victim Assistance Advisor, DoD SAPRO, 4800 Mark Center Drive, Alexandria, VA 22350-1500, telephone (571) 372-2656.

3. Nature of proposed changes for the Office of the Secretary of Defense to the system: The Office of the Secretary of Defense proposes to establish a new system of records to track victim-related inquiries and request for follow-up support services received by the Sexual Assault Prevention and Response Office (SAPRO) via e-mail, SAPR.mil, the DoD Safe Helpline, phone, or mail; to provide for requests for SHL marketing and promotional materials; to allow individuals to provide feedback on the services of a SARC, victim advocate, or other military staff or personnel on their installation/base; to maintain a searchable referrals database that houses contact information for SARCs, medical, legal, chaplain, military police resources, and civilian sexual assault service providers; and to provide user access to the Safe Helpline Reportal Database; to track and facilitate Unrestricted and anonymous notifications of sexual abuse and harassment in Military Correctional Facilities, in accordance with the Prison Rape Elimination Act (PREA).

4. Authority for the maintenance (maintained, collected, used, or disseminated) of the system: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1561 note, Improved Sexual Assault Prevention and Response in the Armed Forces; 10 U.S.C. 1561 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 47, Uniform Code of Military Justice; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; 28 CFR 115.22, Policies to ensure referrals of allegations for investigations.

5. Provide the agency's evaluation on the probable or potential effects on the privacy of individuals: In establishing this SORN, the Sexual Assault Prevention and Response Office

reviewed the safeguards established for the system of records to ensure they are compliant with the DoD requirements and are appropriate to the sensitivity of the information stored within the system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information has been established.

6. Is the system, in whole or in part, being maintained, (maintained, collected, used, or disseminated) by a contractor? Yes.

7. Steps taken to minimize risk of unauthorized access: Victim inquiry records are maintained in a controlled facility that employs physical safeguards including the use of combination locks and identification badges. Access to electronic data files in the system is role-based, restricted to personnel with a need to know, and requires a Common Access Card (CAC) and password. Electronic data is also protected via encryption. The database cannot be accessed from the outside as it does not reside on a server and all records are accessible only to authorized persons with a need to know who are properly screened, cleared and trained.

Follow-up support service records are maintained in a secure, online database. Information is stored in a redundant data center infrastructure with full featured physical security measures, including integrated closed circuit TV and a card reader/biometric security system, man trap security access for raised floor areas, exterior security cameras, and 24/7 security service. Only authorized users who are granted access can have access to software servers, which are housed in three secured cages.

All other records are maintained within the Amazon Web Services (AWS) network infrastructure. The protections on the network include firewalls, passwords, and web-common security architecture. AWS restricts physical access to the data centers where the SHL servers reside. Physical access logs are reviewed and analyzed on a daily basis by AWS personnel. All PII is stored in a password-protected environment with internal access only. All individuals with access to the data undergo a background investigation and sign a nondisclosure agreement.

8. Routine use compatibility: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein

may be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To SAPRO's printing vendor to ship marketing and promotional materials requested via the Safe Helpline.

To the Department of Veterans Affairs to facilitate the resolution of questions regarding benefits and care.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has

been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

9. OMB public information collection requirements:
OMB collection required: Yes.
OMB Control Number (if approved): TBD
Expiration Date (if approved) or Date Submitted to OMB: TBD

Provide titles of any information collection requests (e.g., forms and number, surveys, interviews scripts, etc.) contained in the systems of records: DD Form 2985, “Department of Defense Sexual Assault Prevention and Response Office (SAPRO) Request for Assistance” (OMB # TBD), DD Form 2985-1, "Military Feedback” (OMB # TBD), and DD Form 2985-2, “Materials Request” (collects from less than 10 members of the public per year)

In collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A.

10. Name of IT system (state NONE if paper records only): DITPR # 14355, DoD Safe Helpline; Victim-Related Inquiry Tracking Files

DHRA nn DoD

System name:
DoD Sexual Assault Prevention and Response Office Victim Assistance Data Systems

System location:
DoD Sexual Assault Prevention and Response Office (SAPRO), 4800 Mark Center Drive, Alexandria, VA 22350-1500

Amazon Web Services (AWS), 12900 Worldgate Drive, Suite 800, Herndon, VA 20170-6040.

Social Solutions, 1500 Spring Garden St, Philadelphia, PA 19130

Categories of individuals covered by the systems:
Individuals who request materials or provide feedback on military sexual assault services; sexual assault response coordinators (SARCs), medical, legal, chaplain, military police, and civilian sexual assault responders; Reportable database users; and individuals who call the DoD Safe Helpline or SAPRO for assistance, follow-up support services, or to provide information about sexual abuse and harassment occurring at Military Correctional Facilities under the Prison Rape Elimination Act (PREA).

Categories of records in the system:
For inquiries, feedback, or support requests the following information may be collected: requestor/inquirer's full name or pseudonym, personal/work telephone number, personal/work email address, home address, user type/position (e.g. victim/survivor, family friend, Service member, military spouse, DoD civilian employee, etc.), Service affiliation, rank, base/installation, state, and age; how the inquiry was received (written, email, telephone), type of inquiry (e.g. Army, Navy, Air Force, legal, command, law enforcement, inspector general, medical, Safe Helpline, report of sexual assault, training, etc.), and category of inquiry (e.g. general complaint, criticism of SAPR Personnel or program, general information request, raising a policy issue, report of misconduct, request for Service referral, report of retaliation, praise of SAPR personnel or program); victim's name, Service affiliation, status/position, installation, and inquiry number; installation where the interaction took place, date of incident, the name and/or office and title of the military personnel about which the feedback is being submitted, year assault was reported, if command and/or a

Military Criminal Investigation Office was involved, and case synopsis; documents that inquirer submits to SAPRO; permission for SAPRO to follow up on the inquiry; agency to which the inquiry was referred, agency action officer name, documents sent to or received from relevant agency in support of the inquiry, suspense date, and case synopsis sent to the agency; dates that final status was sent to requester and date the inquiry was closed; comments and dates tracking communication between SAPRO, agencies, and inquirer.

For PREA notifications (information as provided): type of notification (e.g., anonymous report via SAPRO, Unrestricted report via SARC, Unrestricted report via SAPRO, etc.); date and time of notification; location and date/time of the incident; victim's full name (for unrestricted reports); caller's full name (for unrestricted reports); caller's contact information (as applicable); caller's relationship to the victim (self or third party); permission from prisoner for SAPRO to forward the notification for investigation; SARC location and phone number (unrestricted reports only) and details provided by the caller about the nature of the incident (not including PII for all anonymous reports).

For material requests the following information may be collected: first and last name, shipping address, personal or work email, installation/base, rank (if applicable), status/position (e.g., Sexual Assault Response Coordinator (SARC), victim advocate, third party organization, etc.), affiliation (e.g. Service, family member, veteran, etc.), and an open comment field for questions and suggestions.

For the DoD and civilian responders the following information may be collected: name and work-related contact information (installation/base, address, email, phone number).

Authority for maintenance of the system:
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1561 note, Improved Sexual Assault Prevention and Response in the Armed Forces; 10 U.S.C. 1561 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 47, Uniform Code of Military Justice; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; 28 CFR 115.22, Policies to ensure referrals of allegations for investigations.

Purpose:
To track victim-related inquiries and request for follow-up support services received by the Sexual Assault Prevention and Response Office (SAPRO) via e-mail, SAPR.mil, the DoD Safe Helpline, phone, or mail; to provide for requests for SHL marketing and promotional materials; to allow individuals to provide feedback on the services of a SARC, victim advocate, or other military staff or personnel on their installation/base; to maintain a searchable referrals database that houses contact information for SARCs, medical, legal, chaplain, military police resources, and civilian sexual assault service providers; to provide user access to the Safe Helpline Reportal Database; to track and facilitate Unrestricted and anonymous reports of sexual abuse and harassment in Military Correctional Facilities, in accordance with the Prison Rape Elimination Act (PREA).

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside of the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To SAPRO's printing vendor to ship marketing and promotional materials requested via the Safe Helpline.

To the Department of Veterans Affairs to facilitate the resolution of questions regarding benefits and care.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in

response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Electronic storage media.

Retrievability:
Name of the requester, inquirer, or victim; date of inquiry; and/or Military Correctional Facility, as appropriate

Safeguards:
Victim inquiry records are maintained in a controlled facility that employs physical safeguards including the use of combination locks and identification badges. Access to electronic data files in the system is role-based, restricted to personnel with a need to know, and requires a Common Access Card (CAC) and password. Electronic data is also protected via encryption. The database cannot be accessed from the outside as it does not reside on a server and all records are accessible only to authorized persons with a need to know who are properly screened, cleared and trained.

Follow-up support service records are maintained in a secure, online database. Information is stored in a redundant data center infrastructure with full featured physical security measures, including integrated closed circuit TV and a card reader/biometric security system, man trap security access for raised floor areas, exterior security cameras, and 24/7 security service. Only authorized users who are granted access can have access to software servers, which are housed in three secured cages.

All other records are maintained within the Amazon Web Services (AWS) network infrastructure. The protections on the network include firewalls, passwords, and web-common security architecture. AWS restricts physical access to the data centers where the SHL servers reside. Physical access logs are reviewed and analyzed on a daily basis by AWS personnel. All PII is stored in a password-protected environment with internal access only. All individuals with access to the data undergo a background investigation and sign a nondisclosure agreement.

Retention and disposal:
Victim Related-Inquiry Tracking Files (DD Form 2985 and 2985-1): Temporary: Cut off resolved cases files at end of calendar year. Destroy 25 year(s) after cut off.
DD Form 2985-2, Materials Request: Temporary: Cut off completed/canceled request for material at the end of the fiscal year. Destroy 3 months after cut off. (OSD/RDS 101-22)

Responder Database: Temporary: Cut off obsolete/revised records at the end of the fiscal year. Destroy 1 year after cutoff. (GRS 6, Item 14e, N1-GRS-98-2 item
Reportal Administrative Database: Temporary: Close files at the end of the fiscal year after 3 continuous years of inactivity. Destroy 25 year(s) after 3 continuous years of inactivity.
Follow-up Support System: Temporary: Cut off at the end of the fiscal year of close-out of communication. Destroy 25 year(s) after close-out of communication.

All records are destroyed in a way that precludes recognition or reconstruction in accordance with DoD 5200.1-R, "Information Security Program."

System manager and address:
Senior Victim Assistance Advisor, DoD SAPRO, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to Senior Victim Assistance Advisor, DoD SAPRO, Victim Assistance, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

Signed, written requests should contain the name of the requester, the name of the original inquirer, the name of the victim, date of incident and/or Military Correctional Facility, if applicable.

Record access procedures:
Individuals seeking access to information about themselves contained in this system should address written inquiries to the OSD/Joint Staff Freedom of Information Act, Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155.

Signed, written requests should contain the name of the inquirer or victim, the name and number of this system of records notice, date of incident and/or Military Correctional Facility, if applicable.

Contesting record procedures:
The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in

OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories:
Individual.

Exemptions claimed for the system:
None.